

Notice of Allowability	Application No.	Applicant(s)	
	09/875,088	FISHER, DOUGLAS	
	Examiner	Art Unit	
	Jalatee Worjloh	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 4-2-05.
2. ☒ The allowed claim(s) is/are 6-10, 12-31, 33-36.
3. ☐ The drawings filed on _____ are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 6. ☒ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☒ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☒ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material

5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Barton A. Smith (Reg. No. 50,763) on April 6, 2005.

The application has been amended as follows:

1. Canceled.
2. Canceled.
3. Cancelled.
4. Cancelled
5. Cancelled.

6. (currently amended) ~~The method of claim 3~~

A method for conducting authenticated business transactions involving communications using microprocessor equipped devices to communicate over a distributed network, the method being carried out by an on-line authentication service available on the distributed network, comprising the acts of:

- a) enrolling a multiplicity of users with a closed authentication infrastructure, wherein enrolling comprises obtaining and verifying the identity and other

- credentials of the multiplicity of users and providing each user with a unique secret necessary for later authentication to said on-line authentication service and storing the verified identity and other credentials in at least one database;
- b) authenticating a plurality of the multiplicity of users to said on-line authentication service using each user's unique secret to produce a plurality of authenticated users;
 - c) enabling a plurality of groups each group comprising at least two of said plurality of authenticated users to conduct interactions comprising a plurality of messages under persistent mediation of said on-line authentication service, such that each of the plurality of messages passes through said on-line authentication service and is directly monitored by said on-line authentication service;
 - d) wherein persistent mediation of an interaction further comprises the acts of directly compiling an audit trail of an interaction and making the audit trail available to the at least two users in the interaction in an intelligible form at any time during the interaction at the option of the at least two users, and wherein the audit trail comprises at least some of the content of the plurality of messages in the interaction; and
 - e) further comprising the act of providing a discovery portal available to authenticated users through the on-line authentication service such that users can search for other users based on their verified and dynamically variable credentials, whereby users may conduct authenticated interactions with each other without having a prior relationship.

8.(currently amended)The method of claim 7 wherein the act of enabling the plurality of authenticated users to interact with each other in collaboration groups further comprises enabling the at least two users in a collaboration group to make a selection during the interaction of at least part of the audit trail for archival by the on-line authentication service such that it will be held under ~~control~~ of the control of the on-line authentication service for access by any of the at least two users in the interaction after the interaction is complete.

Art Unit: 3621

11. Cancelled.

12. (currently amended)~~The method of claim 11~~

A method for conducting authenticated business transactions involving communications using microprocessor equipped devices to communicate over a distributed network, the method being carried out by an on-line persistent authentication and mediation service available on the distributed network, comprising the acts of:

- a) enrolling users seeking enrollment in the persistent authentication and mediation service, to produce a multiplicity of enrolled users, wherein enrolling comprises obtaining and verifying the identity and other credentials of the multiplicity of users and providing each user with a unique secret necessary for later authentication to said on-line persistent authentication and mediation service;
- b) storing the verified identity and other credentials in at-least one database;
- c) receiving on-line requests from enrolled users for authentication to the on-line authentication service;
- d) authenticating enrolled users seeking authentication to the persistent authentication and mediation service using each enrolled user's unique secret, so as to maintain a plurality of authenticated users;
- e) receiving requests from authenticated users to be connected to particular other authenticated users;
- f) connecting groups of at least two authenticated users under persistent mediation of the persistent authentication and mediation service and enabling the at least two authenticated users which are connected to conduct an interaction comprising a plurality of messages;
- g) repeating act (f) to produce a plurality of groups of connected users;
- h) mediating the interaction among the at least two users of each of said plurality of groups of connected users such that each message in the interaction passes through the persistent authentication and mediation service;

Art Unit: 3621

- i) directly compiling an audit trail of the interaction and making information from the audit trail available to the at least two users of each group of connected users in intelligible form during the interaction and
- j) wherein the act of enrolling users seeking enrollment in the persistent authentication and mediation service comprises the acts of:
 - [[a]]i) distributing software to a user seeking enrollment which enables microprocessor equipped devices operated by the user seeking enrollment to interact with said persistent authentication and mediation service,
 - [[b]]ii) generating a unique private key, and a unique public key for the user seeking enrollment,
 - [[c]]iii) obtaining permanent credentials particular to each of the users seeking enrollment, said credentials comprising public permanent credentials and secret permanent credentials,
 - [[d]]iv) deciding whether to approve the applicant seeking enrollment;
 - [[e]]v) distributing the unique secret comprising the unique private key in the form of a camouflaged private encryption key to the user seeking enrollment if the user seeking enrollment is approved, wherein the private encryption key is camouflaged in a software container, whereby the user's camouflaged private encryption key will generate a correct response to an authentication challenge if a proper access code is entered, but often generates an incorrect but plausible response if an improper access code is entered, whereby if an incorrect response is used notice will be provided to the on-line persistent authentication and mediation service of a security attack;
 - [[f]]vi) distributing the unique public key to the user, wherein said unique public key is in a form which can only be decrypted with a key held under exclusive control of the persistent authentication and mediation service, whereby the persistent authentication and mediation service acts as a closed authentication infrastructure;
 - [[g]]vii) storing said permanent credentials in a customer database, said customer database being accessible to said persistent authentication and mediation service,

Art Unit: 3621

whereby the user seeking enrollment becomes one of said multiplicity of enrolled users; and

[[h]]viii)repeating steps [[(a)]]1 through [[(f)]]vii for each applicant seeking enrollment.

14. (currently amended)The method of claim [[11]]13 further comprising the acts of:

- a) allowing authenticated users to optionally submit variable credentials;
- b) receiving variable credentials submitted by authenticated users;
- c) storing the variable credentials in the customer database according to user;
- d) providing authenticated users discovery software, whereby authenticated users may dynamically discover enrolled users according to search criteria[.]; and
- e) granting authenticated users access to search the public permanent credentials and the variable credentials in the customer database, using said discovery software.

16.(currently amended)The method of claim 15 wherein:

- a) the unique secret comprises a cryptographically camouflaged private key in a software container[.];
- b) wherein the unique public key[[s]] is encrypted with a key held under the exclusive control of the persistent authentication and mediation service and stored in a digital certificate[.]; and
- c) wherein the act of authenticating an enrolled user to the ~~common-authenticating~~ persistent authentication and mediation service further comprises the act of decrypting the encrypted unique public key unique to the enrolled user prior to decrypting the response.

17. (currently amended)The method of claim 14 wherein the persistent authentication and mediation service is provided by at least one host site connected to the distributed network, said at least one host site comprising at least one computer server operated by an open software platform providing intelligent interactions, wherein the operation of the

persistent authentication and mediation service is implemented by software operating on the open software platform.

22. (currently amended) An online service for conducting business transactions among microprocessor equipped devices over a distributed network, the online service comprising:

- a) a host site connected to the network, the host site comprising an open software platform providing intelligent interactions;
- b) a persistent authentication and mediation service, the persistent authentication and mediation service comprising a software PKI authentication agent operating on said open software platform such that communications over the network by said persistent authentication and mediation service are mediated by said open software platform;
- c) a customer database comprising permanent credentials and dynamically variable information corresponding to users of the online service and a database manager for managing the customer database;
- d) software operating on said open software platform which performs at least the following functions:
 - i) enrolling users seeking enrollment in the persistent authentication and mediation service to produce enrolled users,
 - ii) storing credentials corresponding to enrolled users in the customer database,
 - iii) authenticating enrolled users seeking authentication to the persistent authentication and mediation service to produce authenticated users,
 - iv) allowing [[a]] authenticated users to discover enrolled users according to search criteria,
 - v) allowing authenticated users to be connected under mediation of the persistent authentication and mediation service through the open software platform,

Art Unit: 3621

- vi) allowing collaboration between authenticated users which have been connected, and
- vii) memorializing transactions between authenticated users.

23. (currently amended) The online service defined in claim 22 where the function of enrolling users seeking enrollment in the persistent authentication and mediation service comprises the functions of:

- a) distributing software to a user seeking enrollment which enables microprocessor equipped devices operated by the user seeking enrollment to interact with the persistent authentication and mediation service,
- b) generating a unique private key, and a unique public key for the user seeking enrollment,
- c) obtaining permanent credentials particular to each of the users seeking enrollment, said credentials comprising public permanent credentials and secret permanent credentials,
- d) deciding whether to approve the applicant seeking enrollment[;],
- e) distributing the unique public key and the unique private key to the user seeking enrollment if the user seeking enrollment is approved, [[and]]
- f) storing said permanent credentials in a customer database, said customer database being accessible to said persistent authentication and mediation service, whereby the user seeking enrollment becomes one of [[said]] a multiplicity of enrolled users, and
- g) repeating steps (a) through (f) for each applicant seeking enrollment.

25. (currently amended) The online service defined in claim 24 wherein:

- a) the software PKI authentication agent is a pseudo-PKI system of the type which cryptographically camouflages each of the unique private keys in a software container,
- b) wherein each of the unique public keys is encrypted in a form recognizable to the pseudo-PKI authentication agent and stored in a digital certificate, and

Art Unit: 3621

- c) wherein the function of authenticating an enrolled user to the persistent authentication and mediation service further comprises the function of decrypting the encrypted unique public key unique to the enrolled user prior to decrypting the response.

27.(currently amended)A system for conducting business transactions over a distributed network, the system comprising:

- a) a persistent authentication and mediation service site providing a persistent authentication and mediation service, said site connected to the public network, said site comprising
 - i) an open software platform application providing intelligent interactions said platform application mediating all interactions of said persistent authentication and mediation service site via said public network,
 - ii) an authentication agent application comprising a software pseudo-PKI authentication application operating on said open software platform application, said authentication agent application comprising software which enrolls new business[[es]] users producing enrolled users and authenticates the enrolled users producing authenticated business users,
 - iii) an audit agent application operating on said open software platform which logs and monitors interactions mediated by the open software platform, whereby every interaction among authenticated business users passes through the open software platform and is monitored by the audit agent,
 - iv) a discovery software application operating on said open software platform such that said discovery software agent operates to enable authenticated business users to search for other users based on their credentials, and
 - v) a collaboration software application operating on said open software wherein said collaboration software application enables groups of at least two authenticated business users to communicate under direct mediation of the audit agent and to access audit information in an intelligible form during an interaction[[.]];

Art Unit: 3621

- b) a multiplicity of user sites operated by the enrolled users, the user sites being connected to the public network, each site operating at least one computer application whereby it may interact with other business users and each site further comprising software which allows interaction with the persistent authentication and mediation service, a software camouflaged private key, and a digital certificate, said digital certificate comprising an encrypted pseudo-public key encrypted with a key which is under exclusive control of said persistent authentication and mediation service, wherein said camouflaged private key will generate a proper response to a challenge from the persistent authentication and mediation service if a correct access code is entered and may generate plausible but improper responses if incorrect access codes are entered, whereby if an incorrect response is used the persistent authentication and mediation service will be alerted to a security attack on the camouflaged private key; and
- c) a database of authentication information and credentials pertaining to the enrolled business users of said persistent authentication and mediation service, the database accessible to the authentication agent application and the discovery application.

35.(currently amended)An apparatus for providing a service for conducting authenticated business transactions involving a multiplicity of users over a distributed network, the apparatus comprising:

- a) at least one application server connected to the public network, the at least one application server having a computer processor and a computer readable memory, the memory storing the software to implement the service, the software comprising
 - i) an open software platform providing intelligent interactions,
 - ii) a software pseudo-PKI authentication agent application, operating on said open software platform,

Art Unit: 3621

- iii) a discovery software application, operating on said open software platform, and
- iv) a collaboration software application, operating on said open software platform[.,,];
- b) at least one database server, the at least one database server comprising a business users database, the business users database comprising
 - i) authenticated data about registered business users, said authenticated data being protected from user modification;
 - ii) data pertaining to registered business users which is dynamically modifiable by said business users; and
 - iii) data needed for linking business users;whereby the application server facilitates authenticated interactions between business users, including the ability to access other authenticated users without repeated logging in, the ability to dynamically search for authenticated users according to user defined specifications, and accomplish peer to peer collaboration.

36. (currently amended)The apparatus as defined in claim 35 where the distributed network is the public Internet.

Reasons for Allowance

2. The following is an examiner's statement of reasons for allowance:
3. The closest prior art of record is U.S. Publication No. 2003/0095726 to Kia et al.

Kia et al. disclose registering merchants and cardholders with a closed authentication infrastructure. In Kia et al.'s system, registered cardholders are issued certificates containing their public signature keys. A certificate authority verifies the users registration details and store their private signature keys on their computers. During the payment process, theses certificates are used to mutually authenticate the users and to authenticate them to the payment gateway.

Art Unit: 3621

Kia et al. taken either individually or in combination with other prior art of record fails to teach or suggest a discovery portal available to authenticated users through the on-line authentication service such that users can search for other users based on their verified and dynamically variable credentials, whereby users may conduct authenticated interactions with each other without having a prior relationship as recited in independent claim 6, distributing the unique secret comprising the unique private key in the form of a camouflaged private key to the user seeking enrollment if the user seeking enrollment is approved, wherein the camouflaged private encryption key is camouflaged in a software container, whereby the user's camouflaged private encryption key will generate a correct response to an authentication challenge if a proper access code is entered, by often generates an incorrect but plausible response if an improper access code is entered, whereby if an incorrect response is used notice will be provided to the online persistent authentication and mediation service of a security attack as recited in independent claim 12, allowing authenticated users to discover enrolled users according to search criteria as recited in independent claim 22, a discovery software application operating on said open software platform such that said discovery software agent operates to enable authenticated business users to search for their users based on their credentials as recited in independent claim 27 and whereby the application server facilitates authenticated interactions between business users, including the ability to access other authenticated users without repeated logging in, the ability to dynamically search for authenticated users according to user defined specifications, and accomplish peer to peer collaboration as recited in independent claim 35.

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- “Software Smart Cards via Cryptographic Camouflage” to Hoover et al. outlines a method of protecting private keys using cryptographic camouflage.
- WO 99/66436 to Slater et al. discloses a distributed verified trusted third-party system for real-time digital transactions.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jalatee Worjloh whose telephone number is 703-305-0057. The examiner can normally be reached on Mondays-Thursdays 8:30 - 7:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on 703-305-9768. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306 for Regular/After Final Actions and 703-746-9443 for Non-Official/Draft.


Art Unit: 3621

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450

Hand delivered responses should be brought to Crystal Park 5, 2451 Crystal Drive,
Arlington, V.A., Seventh floor receptionist.


Jalatee Worjloh
Patent Examiner
Art Unit 3621

April 7, 2005